360数字安全

数 字 安 全 的 领 导 者

新一代XDR —
面向未来的数字安全防御架构

Gartner

新一代XDR —
面向未来的数字安全防御架构

1. 数字化转型正在重塑未来世界

全球爆发的新冠疫情倒逼各组织（指企业、政府等各个机构）进行数字化转型，如远程办公、混合工作模式，以及云服务等的广泛采用正在成为常态，并且已经永久性地改变着人们的工作、生活和经营方式。对组织而言，数字化转型不仅是简单的业务上云，而是一个推动跨业务、人员、技术等的数字供应链变革的整体解决方案。这种变革正在重塑组织的商业模式，加速业务或商业的数字化进程，增强业务弹性，同时在推动着网络和安全的变革，重塑着未来的世界。

1.1. 数字化转型之业务变革

所谓业务变革，是指随着全球数字化进程的不断推进，在任何地点、任何时间，访问任何应用已经成为数字化业务的基本特征。业务变革的本质是寻求现代IT技术重塑其应用及服务模式，增强业务弹性，持续保持组织在行业中的竞争优势。采用数据中心+云的方式已经成为众多组织IT架构的战略选择，组织的IT领导者正在努力从传统技术堆栈、复杂的IT架构和冗余的供应商中解脱出来，以尽可能低的成本提供即插即用、运营高效的IT服务。比如广泛的利用云计算、大数据、人工智能和自动化等技术不断提升用户体验，逐步减少传统IT系统的投入，加大业务创新，利用和依托数据来做出更加合理和科学的数字化决策，保持业务的可持续性发展，增强业务的敏捷性、弹性和创新性，快速适应各种数字化变革所带来的挑战等。

1.2. 数字化转型之网络变革

网络的本质是提供快速的用户接入体验，缩短用户网络访问的路径，降低网络延迟，简化管理，提升效率。随着组织的业务实现数字化转型，其所带来的最直接的变化是组织的数据不再唯一驻留在本地的数据中心，而是分散在不同的地点，

如公有云、私有云、数据中心、合作渠道、终端、物联网等等。这种复杂的网络直接带来了访问延迟、数据出口成本高昂，用户访问体验差、系统管理复杂、网络成本上升、安全攻击面扩大等众多问题。随着网络不断复杂化，导致大量的数据孤岛出现，进一步加重了组织的IT负担，阻碍了组织的数字化进程。**越来越多的企业把业务迁移到云上，通过互联网直接访问，而不是采用昂贵的专线进行中转。利用互联网，极大的缩短了访问路径，改善了用户体验。**另外，大量的边缘计算网络的出现，让网络的算力更加高效、合理、优化，正在改变着传统网络的格局。

1.3. 数字化转型之安全变革

数字化转型正在颠覆传统网络和安全服务的设计模式。数字时代软件在重新定义世界，一切皆可编程、万物均要互联、数据驱动业务三大特征，给数字技术带来不可避免的安全脆弱性。远程办公、移动办公、自带设备（BYOD）、广泛的第三方SaaS应用访问、第三方影子IT、合作伙伴网络、IT/OT网络融合、开源软件的广泛采用等等业务的变革驱动了网络的变革。太多的攻击载体可以利用，使得攻击者可以轻松的从任何端点、网络到云的任何位置发起。对手可以采用的攻击向量比以往更多、范围更广、烈度更大，从而造成的破坏性更大。随着数字化转型的深入，互联网成为新的企业网络，云成为新的数据中心，传统安全防御的空域、对象、攻击方式等均发生了根本性变化。因此，企业迫切需要新型的数字安全防御思路和手段来应对数字安全新威胁。

2. 数字时代的安全挑战倒逼网络安全行业涅槃

数字时代面临着外部和内部双重安全压力：外部威胁持续升级，造成告警风暴无法应对、高级威胁无法看见、安全事件难以处置等三大困境；内在固有脆弱性难以解决，存在安全人才奇缺、安全技术碎片化、运营流程无法量化改进等三大瓶颈。所有这些都催化网络安全行业即将发生涅槃式变革。

2.1. 传统安全的局限和需求

挑战的背后根因是攻防对抗不可能止于边界。没有攻不破的网络，假定失陷（Assume Breach），敌已在我是不得不接受的现实，在这种情况下，安全的核心是要做到快速看见、快速处置，在攻击做出破坏之前及时斩断"杀伤链"。传统安全建设模式，以安全事件为驱动，通过"堆盒子"来解决问题，当出现某个隐患或热点时，就增加一种设备来应对，尽管传统单点安全产品工具众多，但是集成难度增大，日志难收集，只能依靠进行孤立的数据分析和碎片化安全管理来应对现代系统化的网络攻击。

2.1.1. 无法应对告警风暴

告警风暴，是降低安全运营效率的元凶。一方面，企业数据中心缺乏完善的安全大数据基建。数据中蕴藏着企业风险指标等重要的安全信息。防火墙、IDS、IPS、NDR等各个端类设备上的日志数据格式迥异，语义不统一，难以建立统一的接入方式进行数据采集和规范化处理以挖掘其中的高价值信息。同时调研显示，安全设备日常产生的海量告警数据中，70%以上都是由于业务系统缺乏安全性设计或安全设备检测规则不严谨所产生的误报数据。企业安全人员必需从海量告警中剔除这些误报信息，寻找具有分析价值的攻击告警。利用人工智能和大数据分析技术，实现高精准度的自动化降噪能力，是企业安全运营人员的主要诉求之一。

2.1.2. 无法看见高级威胁

随着高级别专业力量入场，国家背景的APT组织日益猖獗。我国关键基础设施已全面接入互联网和工业互联网，城市、政府部门和能源、金融、电力、交通等重点行业的数字资产成为首选攻击目标。

APT（Advanced Persistent Threat，高级持续性威胁）是一种针对性、隐蔽性、持续性极强的攻击行为，通常会使用加密、混淆或代码重写等高级恶意软件技术来隐藏自身活动，实现长期潜伏的目的。此外，APT攻击组织在识别出核心敏感数据后，会择机将数据转移到外部，窃取数据，更甚者直接瘫痪关键基础设施或接管网站、数据中心等关键资产。现实中的普遍现象是，传统安全产品貌似布防严密却"看不见"APT，导致谁进来了不知道、是敌是友不知道、干了什么不知道。2022年9月，360公司协助国家有关监管部门发布了关于西北工业大学遭受境外APT攻击的调查报告，是印证上述特点的最佳案例。数字时代亟需构建"看见"高级威胁的能力。

2.1.3. 无法高效处置威胁

威胁处置是安全事件运营的最后一公里，威胁处置的速度与质量是成功应对安全事件的关键。威胁处置的过程包括研判溯源、影响面评估、建立优先级处置手段等。而目前的普遍现象是，安全运营人员大多使用人工方式处置威胁：操作多台设备切换不同界面来完成一个威胁处置，如登录平台A看告警，查看服务器B详细数据，封禁防火墙C的IP……威胁处置过程中，受限于多种设备、多种系统，多个安全设备之间的碎片化数据、非标准化技术导致分析研判难、联动与协调难，不同安全事件类型的处置方式选择难，人员技术水平差异导致事件高效处置难。传统的安全处置流程消耗的时间远远超过威胁处置的"黄金时间"，攻击者可能早已"打完收工"。

某案例企业的真实运营数据表明，基于其纳管的120余台安全设备，安全运营团队反复登录多台安全设备进行数据检索和取证，再经由人工进行信息关联分析，作出一次威胁事件的研判论证，平均耗时约3-4天。可以说，传统威胁处置方式已经不能满足当今攻防对抗频次日趋频繁的现实需求。

2.2. 数字时代安全运营迎来变革新诉求

安全运营亟需应对上述安全挑战，而自身又面临安全人才奇缺，安全技术碎片化和运营流程无法量化改进三大瓶颈。每一次科技革命本质上都是通过一个技术创新高效地解决过去一个很费钱或者是投入资源太大的问题。新技术加持下，通过技术来引导管理体系的建设，通过管理保障技术的落地，将人、技术和流程的问题进行整体看待进而寻求系统化设计才能抓住根本。

2.2.1. 安全运营人员存在巨大缺口

据统计，全球信息安全岗位空缺高达数百万个，网络安全劳动力需要在现有规模的基础上增长一半以上才能有效保护组织的关键资产。当前各行业客户的安全团队均存在不同程度的人员缺口。以某城商行为例：人员规模仅3人的安全团队几乎承担着整个数据中心所有的安全工作，包括日常的安全威胁监测分析、安全事件响应恢复、策略规则运营，定期的漏洞检测修复、渗透测试、风险评估，新业务上线前的安全检查，重要时期的安全值守以及年度的安全建设规划等，安全团队工作负荷巨大。

这类现象在中小规模企业甚至是行业腰部企业中屡见不鲜，安全设备建设规模与安全团队人员配比形成巨大的反差，有限的安全人员在繁杂的安全工作中疲于奔命，导致整体安全建设效率低、质量差。

2.2.2. 安全技术不能解决所有问题

新的威胁类型和攻击向量不断催生新的安全技术试图解决某个新问题，如人工智能、大数据分析技术已经越来越成熟地运用到安全场景中，尽管能够有效提高生产力和可见性，但无法完全脱离人的干预。对于复杂高级威胁攻击，最终的研判分析和应急响应仍然依赖于专家能力和经验，而技术的最大价值在于释放专家有限的精力，使其更加聚焦在处理高级威胁攻击，而非海量告警的疲惫处理上。

攻击武器的先进性，攻击手法的隐蔽性、业务场景的复杂化和安全产品品类多样化，促使行业对安全专家的技能水平要求再创新高。企业必须构建一支具备跨域数据分析、事件监控、威胁狩猎等综合能力的团队，才能最大程度发挥设备的生产力，快速精准地处置每一个安全事件，这无疑对行业人员技能培养和企业成本带来巨大挑战，显然，通过SaaS服务的方式按需提供托管运营（MDR）专家服务，越来越多地被企业接受。

2.2.3. 安全运营亟需可量化的持续改进

随着安全建设的持续投入，安全设备的持续采购，安全团队通常会面临不得不回答的灵魂三问：1）我们现在的安全防护能力怎么样？2）我们可以在什么地方缩减预算，在什么地方增加预算，依据是什么？3）之前XX公司发生的攻击事件，我们能抵御么？问题背后的本质是，面向合规开展安全建设，能够回答有或者没有，但面向实战对抗的安全运营，却无法量化衡量运营有效性，最终导致企业无法看到自身的短板，陷入了不知道如何持续改进的痛苦境地。

因此，安全运营亟需可量化的持续改进的机制，满足以下诉求：能够直观地了解网络安全防护能力，安全设备是否如期发挥最大效能，对公司当前的防护水平有量化的认知，清晰认识到安全设备带来的价值和

投资回报率。同时为未来安全设备选型提供可靠数据支撑，检验即将采购的安全设备是否真的有效；从而有效认识安全建设规划及预期与实际效果之间的差距，为未来的规划、建设、优化等决策提供科学量化依据。

3. XDR是面向未来的数字安全防御架构

为了解决「看见」的难题，XDR（Extended Detection And Response：扩展检测响应）作为新兴威胁检测与响应架构一经提出便受到行业普遍关注。XDR产品以"打破安全孤岛，实现有效的检测与响应"的理念为驱动力，来解决数字时代新威胁格局下"看见"威胁的难题。

3.1. XDR的演进

2018年Palo Alto的CTO Nir Zuk创造了XDR这个概念。他先列出客户面对的攻防困境：当时的黑客已经非常专业化，采用的攻击手法多种多样且高度自动化，一旦找出企业暴露面进入企业网络可经过多点跳转入侵攻击目标完成攻击任务。而防守方相比黑客的防护非常死板，靠堆人在几十种安全产品上轮流看告警，这是不可持续的做法，而且不能合力的安全产品一定看不全黑客的攻击面。XDR的核心价值是解决安全产品孤岛问题，整合多个安全产品，把产品的安全数据汇聚进一套集中的大数据平台，并在之上搭建一套安全运营平台及相关服务，自动化地提供检测与响应能力。这个产品价值与解决方案逐渐得到业界的认同。

根据Gartner的定义，XDR是一个安全平台，将特定供应商的多个安全产品，原生地集成到一个统一的安全运行系统中。在Gartner新发布的《扩展检测和响应的市场指南》中，已经将XDR技术扩展至EDR、NDR、SWG、UTM等能力的综合体。XDR中的"X"代表着以终端为起点的安全视野的持续扩展，结合数据湖技术、自动化编排技术及安全分析技术，形成面向多种甚至未知安全场景的综合性安全解决方案。

3.1.1. XDR与EDR

XDR的核心是EDR，因为终端能获得高质量数据，并压倒性覆盖攻击杀伤链的关键技战术，则更直接有效增强了企业「看见」威胁的能力。正如两个名称缩写首字母所代表的，X指eXtended，在EDR外还扩展打通了其他产品。EDR通过实时监测端点上发生的各类行为，采集端点运行状态，提供深度持续监控、威胁检测、高级威胁分析、调查取证、事件响应处置和追踪溯源等功能，及时检测并发现恶意活动。EDR是XDR要对接的最重要的安全产品类别，没有一个好的EDR，XDR的检测与响应效果无从谈起。

XDR以EDR数据为核心，串联跨域安全设备数据，可以更高效地看见威胁并基于攻击链快速做出检测与响应。XDR通过多元异构的大数据关联分析，叠加多层次的AI算法，先把EDR传回的行为数据串接出攻击链的核心，再关联其他检测攻击面的安全产品的行为数据进行延展和合并，最终把包含EDR的多种安全产品的海量行为数据，浓缩成一条清晰的攻击链，并进一步对链上具体的攻击行为提供丰富的上下文，如综合自其他安全产品的资产漏洞信息、大网威胁信息、源自云端数据的攻击者画像等，可以完整的看到安全事件影响的所有资产、漏洞、威胁以及攻击手法，便于按照业务优先级快速处置响应。

3.1.2. XDR与SIEM

从XDR面市的十多年前起，SIEM就是一个非常成熟，稳定发展的市场，和EDR垂直型产品不同，SIEM和XDR同样是广度型产品，如SIEM同样以打破安全产品孤岛的理念，提供从检测到响应的安全运营工作流，甚至具体到多元异构数据分析的技术手段，看起来与XDR高度重叠。XDR作为后起之秀，很自然地参考了当时成熟的SIEM市场产品的功能与技术，尤其借鉴了以大数据和AI为技术突破点，因此两者底层技术上的重叠并不奇怪。

但XDR选了一条更聚焦于检测与响应的从理念到功能落地的路径，我们认为XDR与SIEM产品核心差异点就在于这条路径。SIEM落地时，不经攻防实战方法论指导，不主动挑选合适的安全产品，不定义数据源的质量，而被动得接入所有第三方设备，不加区分地整合，不仅检测效果差，还导致高昂的成本。而XDR以检测效果为导向，选择以过硬的EDR产品为检测与响应的核心，在端点之外依次挑选自家和生态的安全产品，补齐ATT&CK量化统计的攻击暴露面，提供出厂可用，并且部署后仍由云端持续更新的检验与响应内容包，避免客户付出大量安全运营成本

来打通各家安全产品，又能轻松获得专家级安全检测效果。国际主流观点认为，SIEM是客户一站式安全运营的界面，XDR增强了SIEM高级威胁发现能力，SIEM基于这个线索进行分析、溯源和响应。XDR是标品式自动化检测响应，SIEM是人机结合管理和运营，两者珠联璧合，相得益彰。

如何选择SIEM和XDR？首先，我们认为除非是大型企业能投入充足的预算，采购最好的各类安全产品，筹备专业安全运营团队，以完善的安全运营流程来管理，才能让SIEM达到XDR级别的安全检测效果。如果没有一支运营队伍，没有充足的预算，选择开箱即用、快速出效果的XDR才是王道。

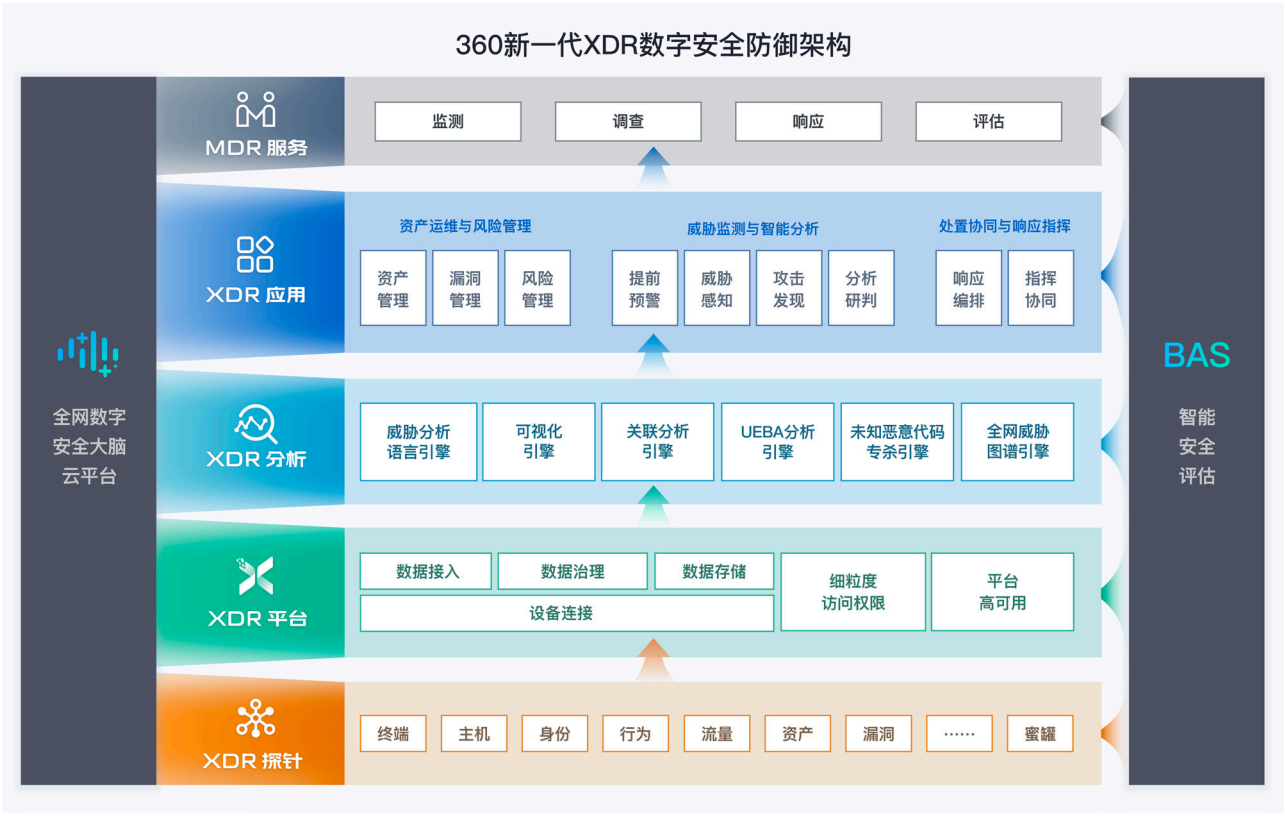
其次，SIEM和XDR并不互斥，功能可以相互补充，在客户处共存。多数XDR厂商，相比SIEM厂商追求功能的广度，只做自己最擅长的检测与响应领域，刻意做了减法，会缺乏一些SIEM产品具备的其他领域的功能，比如审计合规、与各种企业的管理类软件对接等等。此类需求，可以由XDR产品和SIEM产品组合使用来实现。在未来一段时间内，预计安全预算充足的大型企业，仍然会同时使用SIEM和XDR。

3.2. 新一代XDR的模型框架

数字化转型将网络安全上升为数字安全，新一代XDR依然坚定不移地以"打破安全数据孤岛，实现有效的检测与响应"的理念为驱动力，持续提升数字时代新威胁格局下"看见"威胁能力和对抗效率。因此，新一代XDR技术拓宽了分析范围，可关联分析更多维的遥测数据（终端、网络、云端、移动端、邮件、资产、浏览器、蜜罐等），整合更多元威胁数据（全球威胁情报、资产、漏洞、暴露面信息等）和专家知识库（APT基因库和攻防知识百科等），将会与资产以及全网情报数据深度结合，并向云地一体化运营转变，将"看见"威胁的不确定性进一步依赖云端以更广视野，更大资源和更强能力解决，进一步更快、更全的看清攻击杀伤链。托管检测和响应（MDR, managed XDR）可以最大限度提升安全运营效率效能。最终，助力安全回归到"攻防对抗"的本质上来，做到"知己知彼百战不殆"。

图1

360新一代XDR数字安全防御架构



资料来源：Qihu

3.2.1. 新一代XDR与ATT&CK攻防知识百科

想要打造出一款真正有效的XDR产品，更高效地解决「看见」的问题，数据质量是一切的前提。数据已经成为了数字经济的关键生产要素，在安全的语境下，数据驱动安全在安全行业中也已成为共识。但在数据驱动安全的背后，数据的质量显然成为了关键成功因素。换而言之，当采集数据这件事情变成共识的时候，采集什么数据就变得至关重要，准确全面的数据决定了后续分析能力效果的上限，如果对于到底要采集什么样的数据没有清晰的洞察和认知的话，就会陷入一个误区，让一堆的无效的垃圾数据占据大量的计算资源，几乎无法从中发现有效的信息。

因此，我们认为从实战中沉淀攻防知识，由知识定义XDR数据标准，是XDR达到良好检测和响应效果的必要条件。也就是说要为XDR建设一套指导数据收集、分析、响应、评价的维基百科，我们称之为攻防知识百科。这套知识百科指导XDR建设方案需要接入怎样的数据源，如何去做检测分析，如何准备应急预案，如何做效果评价，进而形成了一套将攻击知识转换为防御策略的方法论和产品验证的方式，最终真正地做到对威胁的看见和处置。想要做好这件事不简单，需要在安全大数据、知识库、安全专家方面的持续积累，将全网视野看到的APT攻击、黑客渗透、恶意软件等多种威胁事件分门别类地进行了梳理和沉淀，将实战攻防对抗中新增的攻击技战术、攻击活动杀伤链、攻击工具、攻击者组织信息、所涉资产类型、所涉数据源、检测规则、防御方案等信息，以及它们之间的关系都呈现在一个可视化图谱上，让安全研究和运营人员全面全覆盖看到实战攻防技战术全景，并建立攻击、防御和评估之间的"相互关联性"，形成XDR实践的明确行动指导。

3.2.2. 新一代XDR与安全大数据

XDR是数据质量与规模质变而激发的能力质变。无论采集多少数据，一个企业内部仅可以形成具备自我视角的"小数据"，具备全行业乃至全国视角的

图2

360 APT基因库和攻防知识百科-攻击、防御、验证知识库内容

资料来源：Qihu

真“大数据”是企业难以实现的。只有“小数据”+真“大数据”相结合，才是XDR未来的解决思路。

如何实现“小数据”+真“大数据”结合，简单说来包含两个要素：一个本地化安全大数据平台用以负责存储和计算客户的“小数据”，一个全网安全大数据连接器用以获得更多的“全网大数据”加持，全面赋能安全分析与响应。这样从架构上打破云端知识、客户业务及威胁数据之间的固有屏障，融通各类安全数据，协同整体实战决策。

安全大数据平台具备海量大数据实时处理能力，根据数据规模能够扩展至百万EPS大数据处理能力，支持跨数据中心的全局关联分析，其在流量，资产，进程，网络，内核行为等各个安全子领域定义了专用的XDR数据模型，能够快速接入各类XDR数据使之集中管理，并在内部融合数据品类，协调数据流程决策与步骤，为安全业务提供从数据接入到存储、清洗到运算，最终到威胁发现一站式开箱即用的服务。相比通用化的大数据平台，其数据处理能力更专业，其安全分析功能更丰富、性能更高、部署和运维成本更低。

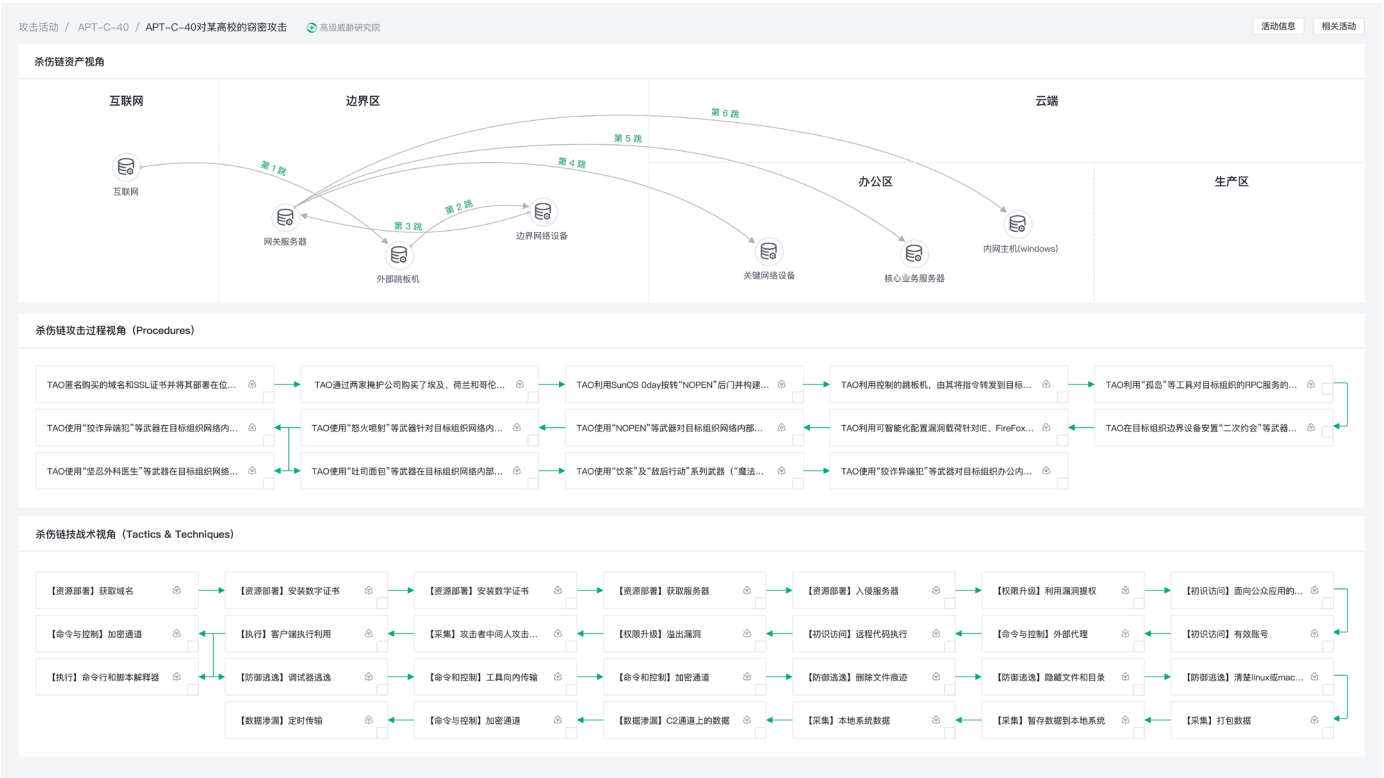
云端赋能连接器连接全网大情报数据，为XDR分析提供从漏洞到资产、从情报到知识、从线索到规则、从事件到态势等100余种基础的安全数据及分析的赋能，活动与攻击者画像相关的一切信息，助力安全运营人员在攻击事件中抢到先机。如：失陷事件检测、攻击来源识别、恶意样本鉴定、风险URL检测、漏洞排查分析、文件信誉评分、风险资产测绘、战术战法还原、高级威胁检测、威胁图谱分析、人工智能分析等。

3.2.3. 新一代XDR与人工智能

面对海量的威胁数据，人工智能机器学习技术可提升网络空间威胁检测、响应能力。基于网络空间大数据提供的数据资源，机器学习技术提升了网络空间感知与防御手段对于各种不确定性环境的动态适应能力，能够对海量模糊、非线性、异构数据进行自动化的

图3

360 APT基因库与攻防知识百科-攻击杀伤链资产视角与攻击过程视角



资料来源：Qihu

分类聚合与关联分析，全面感知识别网络安全威胁，自主学习认知网络空间态势；能够主动生成与快速调整网络威胁防御响应策略，在与自主化、智能化网络空间攻击手段的攻防博弈中不断学习演进，逐渐形成适应性强、反应迅速灵敏的网络空间安全防御"安全大脑"。

XDR平台应内置多种机器学习赋能的检测、分析引擎，支持进行样本检测、威胁情报检测、终端异常行为检测、网络异常行为检测、资漏关联分析、多维度关联分析、自动化溯源分析等多维度检测分析手段，可有效识别高级未知威胁并自动响应应对。

3.2.4. 新一代XDR与威胁图谱（Threat Graph）

安全专家在面对攻击的复杂性，他们需要有足够的技能和聪明才智，而威胁图谱技术是XDR加速调查响应，遏制攻击的关键技术。威胁图谱技术通过应用图分析和机器学习算法的组合，有效地建立主机、用户、内外网IP、域名、文件、进程等实体之间的关系和行为，提供了对客户环境所有端点、网络、用户、应用数据的完全实时可见性和洞察力。例如对于一个文件实体，通过威胁图谱技术可以找到它的访问域名、访问IP、访问用户、关联漏洞、关联样本、代码执行行为、访问行为，且都时序地展现出来。更难能可贵的是，所有的实体及实体间的关系，都呈现在一个统一的视图和操作界面，安全专家可以非常方便的基于事件的关系、上下文、序列来确定攻击是否正在进行，并直接在实体上进行分析和处置。这些实体之间本不直接相关，但可能构成潜在攻击，采取其他方法将难以被发现。

利用威胁图谱，客户实现了在攻击发生过程中阻止攻击，这与事后溯源取证完全不一样。没有威胁图谱之前，安全分析专家往往通过添加情报源，编写关联分析规则，试图将多个数据源的数据进行反复透视，以确定事件之间的潜在关联，找到线索，这实质是个

图4

全网安全大数据赋能客户安全运营

资料来源：Qihu

劳动密集且门槛很高的过程。这种类型的调查，通常需要数小时甚至数天的时间，占用了宝贵的安全人才和资源。但威胁图谱存储了所有攻击活动的时间线、所有关联的实体关系全部呈现在一张图上，客户可以在威胁图谱上进行快速调查分析、判定优先级，判定影响面、响应处置，这个过程可以在几分钟内完成，从而比对手赢得宝贵的时间。

充分利用云端威胁图谱能力可以指数级提高检测响应的速度和精度。云端威胁图谱利用强大的图分析功能实时搜索数十亿事件，在全球级的数据量上建立安全事件之间的联系，以规模化和前所未有的速度快速检测和预防全球黑客攻击。如果威胁图谱在一个客户环境中检测到某些东西，所有客户都会自动从中受益。例如在单个客户站点上发现的一个新的实体、攻击技术、攻击工具可以立即连到全网数据中进行测试和验证。利用云端威胁图谱的"百亿节点千亿边"的规模和数据生产速度，快速检测新型未知攻击，显著提高检测响应的速度和精度。这相当于在用全网的力量和专家集体智慧在帮客户检测一个未知威胁。

3.2.5 新一代XDR与SOAR技术

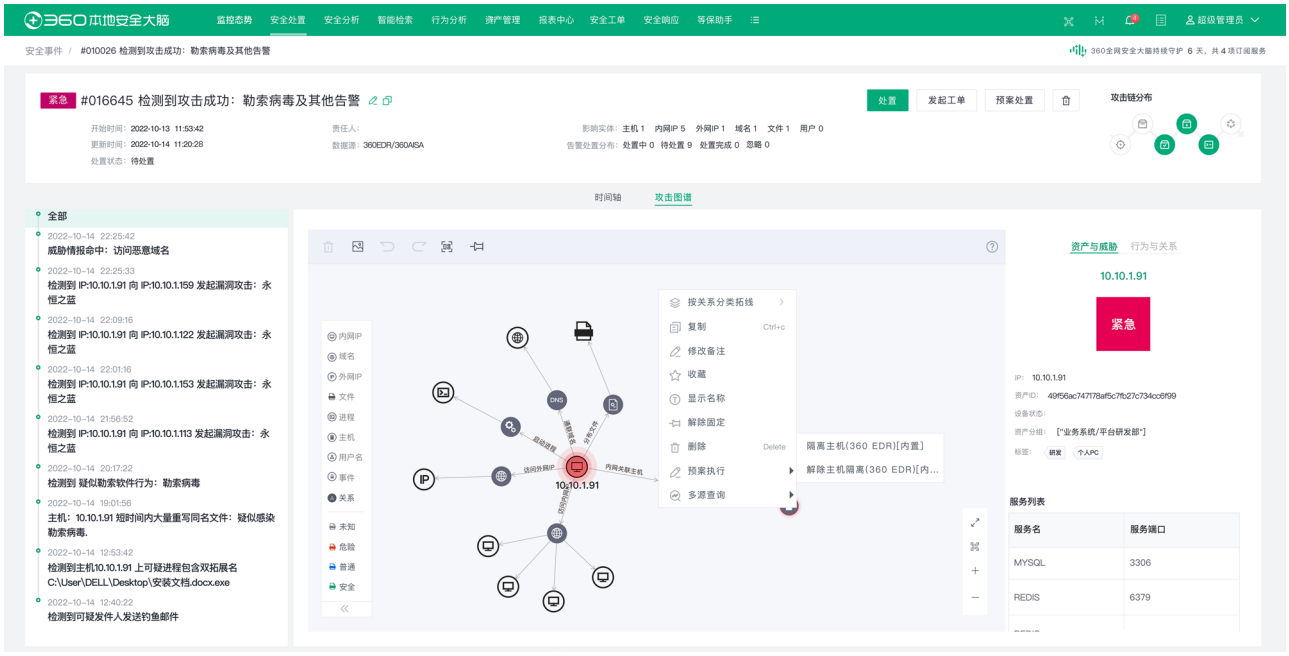
XDR中的R是指"响应"，这意味着在识别出威胁后，需要尽快进行响应和处置。所以，响应和处置是XDR的必备技术。而SOAR恰恰是快速响应和处置安全事件和威胁的重要法宝。据调研，93%的安全专业人员认为他们的SOAR对于复杂的安全运营流程和基本的安全运营任务都是有效的。

下一代XDR通过集成SOAR组件，可以更加高效地实现安全编排、自动化和响应，可以让安全团队通过同一个控制台立即消除网络、端点和云威胁。SOAR可从XDR工具中获取告警，利用上下文和情报自动富化，并根据风险评分对安全事件队列进行优先级排列，结合开箱即用或自定义剧本，实施最佳实践安全流程，加快客户的调查和事件响应时间，提高安全运营团队的效率，使得安全运营流程标准化。

然而，由于编程技能不足、安全运营流程不成熟等原因，SOAR的价值尚未得到充分体现。为了帮助客户开启SOAR之旅，应该从常见的场景用例开始启程，比如自动化网络钓鱼响应、自动化恶意软件分析等场景。通过将各种场景用例的自动化内容包和预构建集成打包在一起，就可以引导客户快速入门。

图5

威胁图谱富化拓线分析助力调查响应



资料来源：Qihu

3.2.6. 新一代XDR与MDR服务

新一代的XDR产品在解决"看见"威胁问题的同时进一步促进托管检测和响应（MDR，managed XDR）服务进化，MDR服务将客户本地XDR数据和全网情报大数据深度结合，配合不间断的安全专家级监测、调查和响应服务，将"看见"威胁的不确定性进一步依赖云端以更广视野、更大资源、更强专家队伍解决。在全网安全大数据赋能下，安全专家团队能够帮助客户看到全局，而不仅仅是恶意活动在单个组织内部的片段，还可以通过专家实战经验更快的溯源发现未知的新型威胁以及定向的APT攻击，这样可以最大限度的减少威胁带来的风险和影响。

XDR的安全托管MDR服务应用落地，将从"事前安全专家级监控预警"、"事中定位网络安全攻击所处阶段、安全专家协助处置"、"事后归纳总结，结合安全专家建议和安全大数据分析指导未来网络安全建设方向"这三个层面提升了客户的安全能力，而客户付出的成本远远小于组建一支安全专家团队，MDR服务是短时间内解决网络安全专业人员的短缺和相关技能差距的有效办法。

3.2.7. 新一代XDR与BAS技术

如果说XDR是ATT&CK攻防知识百科指导下的一类聚焦检测与响应工程化的产品，那么BAS（Breach and Attack Simulation）是ATT&CK攻防知识百科下聚焦有效性评价的另一类工程化产品。XDR和BAS通过同一套知识体系赋能，让数据接入、检测、响应、评价形成统一的度量标准，换言之，我们认为BAS是XDR的伴生技术，是检验XDR技术有效性的评价手段，更是指导企业安全运营持续改进的量化标准。

在没有BAS之前，安全有效性评价高度依赖安全专家个人能力和经验，需要某一个人来指出，当前哪里存在风险需要加固、发现了哪几个高危动作可能存在攻击风险等，这中间存在主观性、时间成本、人力成本等不确定因素。BAS带给XDR的价值是，当一次新的攻击事件发生后，能够迅速地通过灭活重放的方式做自动化、持续性、常态化的覆盖性评测，去验证当前的XDR防御力量到底够不够强大？是不是每一个XDR探针都采集到了它需要的数据，XDR规则检测到了它需要检测到的攻击？如果没有，我需要补充什么样的能力到XDR体系？难能可贵的是，这不是定性的评估，而是定量的评估，BAS为XDR有效性提供有的放矢的数据支撑，就好比一双去伪存真的试金石，XDR效果好不好，BAS测一测便知道。

3.3. 360 XDR最佳实践

360 XDR拥有精准全面的XDR探针，全网安全大脑赋能的安全大数据及智能检测响应能力。通过XDR客户可以获得更好的威胁看见能力，更快速的分析响应以及最大化的投资回报率。可适用于大中型企业提升对高级威胁的检测与快速响应；也可适用中小企业、县市级政府机关、医院、大中院校等中小规模客户，产品开箱即用使用简单，同时搭配安全服务体系，日常安全合规、告警处置简单易用，重大事件专家快速响应，全面提升安全运营效率。

3.3.1. 核心优势

一个优秀的XDR方案，是终端安全技术、大数据处理技术、大数据分析技术、AI人工智能技术、智能安全评估BAS技术、APT基因库和攻防知识百科、安全运营和对抗专家服务有机整合发展到高峰的自然成果。360在这7个方面积累了长年的核心优势：

EDR上高质量事件的捕获能力：数据采集质量决定了EDR真正的检测效果，采集高质量的安全数据是终端安全最有难度的工作之一。高质量数据第一强调采集维度，多维度的大数据才是真正的大数据。360 EDR支持最全维度数据采集，时间维度包括攻击前，攻击中，攻击后；行为维度包括标准行为，差异行为，破坏行为；阶段维度包括有感染前，感染中，感染后等，只有这样的大数据才是高质量数据，基于高质量的数据才能真正发挥EDR的检测效果。高质量数据第二强调采集精度，360 EDR使用360十几年积累的内核分析技术、核晶硬件虚拟化引擎等多种引擎来收集安全数据，直接抓获内核漏洞利用的行为，实现最精准采集；360 EDR提供超越内核级监控能力，利用CPU的硬件虚拟化机制增强64位系统的安全防护，对进程创建、进程注入、模块加载、注册表值写入、文件写入等等行为进行全面监控，有效对抗APT绕过攻击。这些都是360 EDR独一无二的核心技术。

全网安全大数据：大数据作为360 XDR的持续驱动力，能够实时同步全球威胁，持续增强对APT攻击的检测和感知能力，在全网范围内对安全事件做快速关联分析。基于17年实战经验，360已汇集了超300亿程序文件样本，22万亿安全日志、90亿域名信息、2EB以上的安全大数据，每天新增1.5 PB，可瞬间调用超过百万颗CPU参与计算、检索和关联多维度威胁数据。

运营商级大数据处理及灵活低代码分析技术：安全大数据平台具有"运营商"级别的数据处理能力，并支持高速对接Hadoop/Spark生态组件进二次算法或编程式分析；自研的运营商级别的流式实时分析引擎，每秒处理事件性能超过100万，且能实现跨多数据中心统一分析。通过三层索引、列式数据压缩和概率文本索引技术，对历史数据的各种搜索，即使在PB级数据规模下，都能超出各类开源产品的15倍以上，而在实际部署上，运行这些功能，只需要同类平台的1/6机器配置。内置解析规则支持接入200+厂商，2000+数据源，输出多达1200+解析维度，是业界数据解析最规范和全面的平台。

AI人工智能技术：360 EDR拥有静态样本检测的QVM，从使用早期支持向量机、随机森林等算法，到使用AI研究院自研算法，是成熟的新一代人工智能反病毒引擎；雷鸟引擎则是针对EDR所采集的时序事件进行分析，既包含经验规则匹配，又利用长短期记忆网络等深度学习方法训练与检测。XDR分析预置了10大类，60余小类，2000多个安全规则，应对纷繁复杂的安全业务，可灵活组合、相互补充、协同联动，支持机器学习，自研关联关系算法等十余种检测模型，集合XDR数据和全网威胁大数据能有效识别用户异常操作、高级未知威胁并自动响应应对。

创新智能安全评估BAS技术：360 XDR创新性地引入国际领先的入侵和攻击模拟BAS技术，通过订阅360 APT基因库和攻防知识百科，采用实战化、无害化方式模拟攻击，持续性地对客户布防的安全设备进行全面覆盖性测试，以度量其面向历史及最新攻击的整体效能和差距。系统内置数千评估用例并每日更新，ATT&CK技战术已覆盖达70%以上，支持WAF、IDS、IPS、APT流量、NDR、EDR、EPP、邮件安全网关、HIDS、DLP等安全设备评测，支持对主流场景APT、勒索、挖矿、紧急高危漏洞等安全体系的整体防御能力评估。360 BAS提供场景编排功能，以图形化、流程化的方式展示一次攻击活动的上下文，通过完整的攻击链呈现一次攻击活动中所使用的技战术，通过包含完整上下文的攻击场景，全面评估安全产品对完整攻击的防护情况。可随时发起安全评估任务，一键生成安全评估报告，为客户提供针对性的改进建议，帮助量化评估并持续改进纵深防御体系有效性。

360 APT基因库和攻防知识百科：360通过十年累积，已经拥有APT排查规则数百条；TTP技战术规则近千条；沙箱检测规则数千条；还原杀伤链检测规则数万条，黑白名单250亿左右。同时拥有50多个知名APT组织的攻击信息，这些信息不仅涵盖了业界流行的MITRE ATT&CK攻防知识库，而且基于360的实战经验在此基础上做了大量补充。保持更新扩充的基础上，将网络攻击技战术、攻击工具及攻击者组织等信息，用规则和知识的方式提供给客户，为用户基于已知威胁对抗未知威胁提供明确而强大的行动指导。

世界顶级安全运营和对抗专家服务：360拥有具备顶级漏洞挖掘能力的东半球最强白帽军团。至今为止，360专家已成功挖掘谷歌、微软、苹果等主流厂商CVE漏洞近2000个，包揽三巨头史上最高漏洞奖励，并已成功追踪溯源海莲花、摩诃草、美人鱼、蔓灵花、蓝宝菇等针对中国的境外APT组织累计多达50个。在持续与各国高级别黑客较量过程中，淬炼出了一套业界独有的"实战兵法"，并以此赋能指导360 XDR实现对各种威胁进行溯源分析及提供相应的解决方案。

3.3.2. 典型应用场景

政府政务迅速向数字化转型升级，网络安全既是业务的支撑能力，也是业务保障发展的前提。360与重庆、天津、青岛、苏州、上海等市政府合力打造360城市安全大脑，以360终端、流量、测绘、大数据等数字安全能力为抓手，基于XDR架构向城市企业提供基于"看见"为核心的一站式城市安全运营平台，通过帮助城市、政府、企业客户打造的集态势感知、指挥控制、通报预警、信息共享、应急响应为一体的安全运营体系，构建"摸清家底、感知风险、看见威胁、处置攻击、提升能力"5大安全能力，形成面向数字安全复杂威胁的完整应对能力。

360城市安全大脑基于XDR技术框架为用户提供持续监测、深度调查、快速响应的MDR服务：

- 监测：安全专家基于城市XDR平台的能力输出，提供持续的（24x7）的关键警报监控和事件关联分析，并对其做响应优先级排序，优先处理高危威胁，快速发现快速响应。
- 调查：安全专家通过溯源分析，构建攻击的全貌。帮助城市托管用户在追踪威胁时理清攻击链，了解攻击者与其使用的攻击技术，分析影响面，选择正确的应对措施和加固方案。
- 响应：安全专家通过主动通知城市托管用户或主动调用XDR产品的响应处置功能，及时处置威胁，阻止攻击进一步扩散。并下发安全情报、策略，以防未来的攻击。帮助客户及时处理，降低影响。

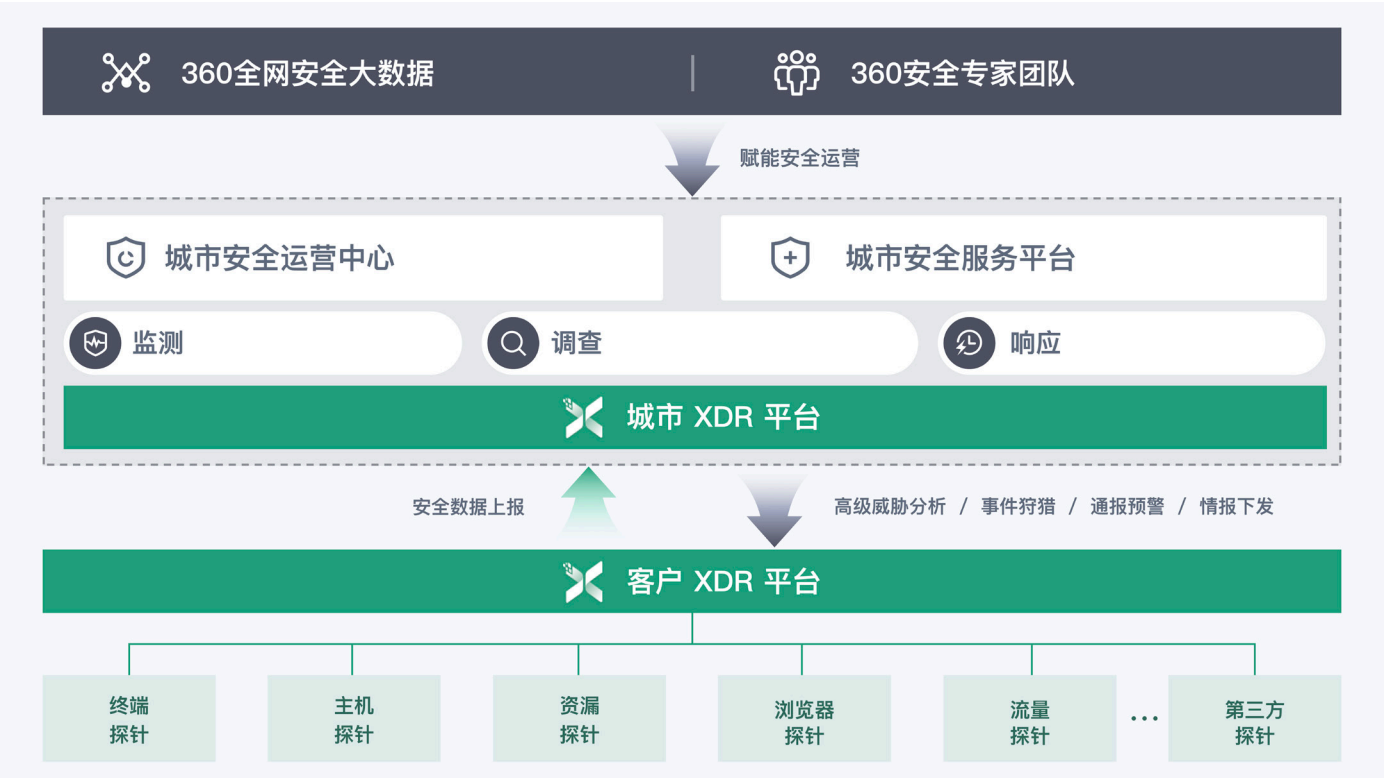
3.3.3. 典型威胁检测案例

360XDR作为新一代的网络安全解决方案，可从终端、网络、浏览器等多个来源收集数据，并基于从海量攻防数据中抽象出的威胁模型，进行自动化的高级威胁检测和响应处置。

以"酸狐狸事件"为例，终端探针设备，采集终端上的进程、文件、注册表以及敏感API调用等遥测数据，识别恶意软件的植入、劫持、上传数据等行为；流量探针设备，通过采集网络会话的元数据，识别异常流量，发现诸如中间人攻击、下载恶意软件以及外连命令控制服务器等行为；360XDR可进一步关联终端和流量数据，分析还原整个攻击链路，方便安全团队研判；同时能自动化提取威胁攻击IOC和标记受害资产，预置的自动化预案自动调度防火墙对C2地址进行封禁，调度终端防护系统扫描受害主机隔离恶意文件。通过部署360XDR，企业能有效提高威胁

图6

360城市安全大脑



资料来源：Qihu

图7

360 XDR检测高级持续性威胁

资料来源：Qihu

检测精度，大幅提升安全运营的效率，缩短MTTD和MTTR。

3.3.4. XDR客户收益

降低安装和维护成本、简化调查分析降低运营成本。360 XDR是一站式安全运营平台，整合终端、网络、云端360自研产品和生态产品，简化部署和管理，将以往需要几周完成的安装部署和设备对接工作降低到1天完成，实现开箱即用。360 XDR根据预置规则动态地将终端、网络和云端数据整合在一起，准确识别特定于每个客户环境的威胁并生成完整的攻击链路，大大减少了安全专家人工手动搜索进行分析溯源的时间，从半天时间减少到十几分钟，分析溯源效率成倍提高，大幅降低运营成本。

避免运营门槛和学习使用成本。360 XDR提供开箱即用的威胁检测和行为分析检测规则将近500条，无需到客户环境构建检测策略就能够立刻发挥价值，降低策略调整的运营成本。云端专家也在持续的运营优化这些规则并定期更新，确保规则的效果持续提升，大幅度降低安全团队人员学习与使用成本。

提升检测率和检测效果。360 XDR以APT基因库和攻防知识百科为指导，关联分析多维神经元数据，结合资产、漏洞、威胁情报等多元信息，精确识别攻击行为并聚合为安全事件，将待处置的告警量降低2-3个数据级，极大的减轻了安全团队人员应对海量告警的

工作负荷。在处置响应环节，360 XDR预置了上百套SOAR协调指挥预案，利用自动化引擎快速进行安全事件处置，平均处置效率提升至10倍以上。

4. XDR的未来演进

随着数字化技术的不断发展，数字攻击面正在不断扩大，对手使用比以往更复杂的技术，无论是在攻击的范围、攻击的速度，还是在针对性和破坏性方面都在不断演进。传统的单点安全技术工具正在形成新的安全孤岛，如传统VPN等甚至成为攻击者的攻击目标。传统安全工具产生的越来越多的报警使得安全运维团队筋疲力尽，海量的报警淹没了真正重要的安全风险，为对手创造了更多的攻击机会，导致防与攻的差距不断拉大。

未来的XDR的演进将主要体现在三个方面。

一是未来的XDR将更加开放。未来的XDR将通过对所有安全操作中的事件进行管理，并提供持续监控和分析，为零信任计划的实施提供原生的决策支持。如未来的XDR将设备和身份会统一关联，打破对手所依赖的数据孤岛，从不断分类和调查单一零碎的安全报警，转向跨越云工作负载、电子邮件、端点、网络、OT/IoT、身份威胁分析等更广泛的应用场景及其数据源的支持；未来的XDR将利用云计算、边缘计算、数据湖仓、人工智能和专家知识等的有机融合，遵循零信任理念、围绕检测、取证、响应、威胁调查等全生命周期，来构建智能检测、威胁评估、主动响应、前沿防御的弹性安全防御体系；未来的XDR将提供统一和自动化的安全方法，迅速评估威胁并采取措施，从而实现更快、更有效的威胁检测和响应。360多年以来在云端发力成功实践了基于海量大数据、威胁情报以及机器学习能力和云计算框架支持的原生XDR技术，同时为企业提供基于SaaS的云原生XDR服务。相信随着数字化转型深入，国内大多数企业会逐渐拥抱云原生的XDR技术和服务。

二是未来的XDR将建立社区防御框架。为了应对对手对软件供应链越来越严重的攻击，未来的XDR将更积极的发挥社区的力量，跨越应对单一客户面对的安全威胁到社区的联合防御，将会定义和推广最适合最终用户的开放式XDR框架和架构;未来的XDR将帮助SecOps团队更好的集成不断出现和发展的各种应用程序、安全网络技术等，保护客户已有的安全投资，并能实现所需的安全功能的原生化的持续增值；未来的XDR开放框架将鼓励社区力量进行联防，鼓励提供开放式XDR和大数据分析、威胁检测、攻击面管理、调查和响应等标准框架支持；该框架也将更广泛的与托管安全服务提供商（MSSP）、托管检测和响应服务（MDR）以及系统集成商（SI）等进行合作。

三是未来XDR将超越技术本身，而是一种主动防御的思想和哲学。XDR是一种哲学，它基于安全应该始终关联数据并在整个数字安全空间中持续检测和响应；XDR必须建立在端点检测和响应(EDR)的基础之上，因为端点是数字安全空间的入口，也仍然是最有价值的安全数据来源，未来的XDR一定要以最好的EDR作为基础；未来的XDR将从对手的视角出发，以结果为导向，以运营为中心，打破对手藏匿的筒仓和传统安全工具的孤岛，针对威胁而不是报警不断优化快速"看见"和极速响应能力的方向不断演进；未来的XDR将整合威胁情报、零信任架构，可以跨云和本地环境为客户交付现代化速度和规模化的安全运营和分析服务；未来的XDR可能会嵌入到组织的数字业务的每一个组成部分中，以数据的价值为中心，基于数据的全生命周期的价值流转，成为构建原生安全基础设施；未来的XDR将不会取代现有的某一个安全工具和技术，而是会超越现有的安全模式，体现主动防御、极速响应、规模化安全服务的思想和哲学，重新定义安全，帮助客户构建更全面、更高效的风险管理计划，重塑数字安全的底座，加速组织的数字化转型进程。

资料来源：Qihu

Gartner的研究：

2022年预测：整合式安全平台将是未来的发展趋势

服务要求日益繁多、威胁态势快速变化、技术人才匮乏……在此背景下，安全和风险管理负责人依然需要"以少博多"。本研究预测，平台整合将帮助安全和风险管理负责人所在组织在恶劣的环境中蓬勃发展。

概述

主要发现

- 在降低复杂性、利用共性和最大限度减少管理开销的需求驱动下，安全技术正在跨越多个学科领域加速融合。
- 企业正在制定或计划制定供应商整合战略，由于涉及大规模的架构转变，这对大多数企业来说都是一个长期任务。
- 供应商日益分化为"平台"和"组合"两大阵营，前者整合多种工具，使之成为一个大于各部分之和的整体，而后者则将产品打包，很少整合。
- 技术整合并不局限于一个技术领域，甚至不局限于一组密切相关的技术，而是在许多安全领域并行发生。

建议

- 评估共享数据和控制平面的安全平台；利用这种整合来定义常见政策，并减少传统孤岛之间的差距和漏洞。
- 评估您对出站通信的安全需求，并确定云管理的解决方案在哪些方面契合您的风险和业务情况。
- 清点数据安全控制措施，当您需要利用您的数据来支持现代数据安全平台时，孤立的数据安全工具会阻碍行动，因此您应该在几年的时间内逐步淘汰这些工具。
- 实施集成和融合的安全方法，涵盖云原生应用从开发到生产的整个生命周期。
- 作为降低安全运营复杂性的一种有效方式，评估由扩展检测和响应统一起来的工作空间安全包。

战略规划设想

到2025年，80%的企业将实现从单一供应商的安全服务边缘(SSE)平台统一网络、云服务和私人应用程序访问。

到2025年，由于对更高级别的数据安全的需求被压抑，以及产品功能的迅速增加，30%的企业将采用数据安全平台(DSP)。

到2025年，70%的企业将把保障云原生应用程序生命周期的供应商数量整合到最多三个供应商。

到2027年，50%的中端市场安全买家将利用扩展检测和响应(XDR)来推动工作空间安全技术的整合，如端点、云和身份。

分析

企业需要了解什么

安全技术和观念一直在同类最佳解决方案和平台解决方案之间摇摆不定（即使后者经常是一种营销手段，而不是实际方法）。这种摇摆是由采购中心、供应商偏好和技术需求所驱动的。它给企业和安全与风险管理(SRM)领导者留下了巨大的技术债务，而且往往是一个分散、复杂的基础设施，无助于企业实现其数字业务的使命。这种基础设施难以管理，影响对真实安全状态的判断，还会造成孤岛之间的差距或政策不匹配。

Gartner的2020年安全和IAM采用趋势调查1表明，大多数企业已经或计划制定供应商整合策略（见图1）。只有20%的企业不打算采用这种策略，而在已着手部署策略的企业中，超过80%的企业已经实施了至少一年。

这并不是我们第一次看到在统一平台上整合供应商这种趋势-情况已经多次反复。虽然这种模式将继续下去，但我们今天的情况有所不同-一方面是复杂的、非整合的成套产品带来的负面影响，另一方面是整合所能带来的积极协同作用。现代平台跨越常见的数据和控制平面，并使用云技术来综合海量数据。

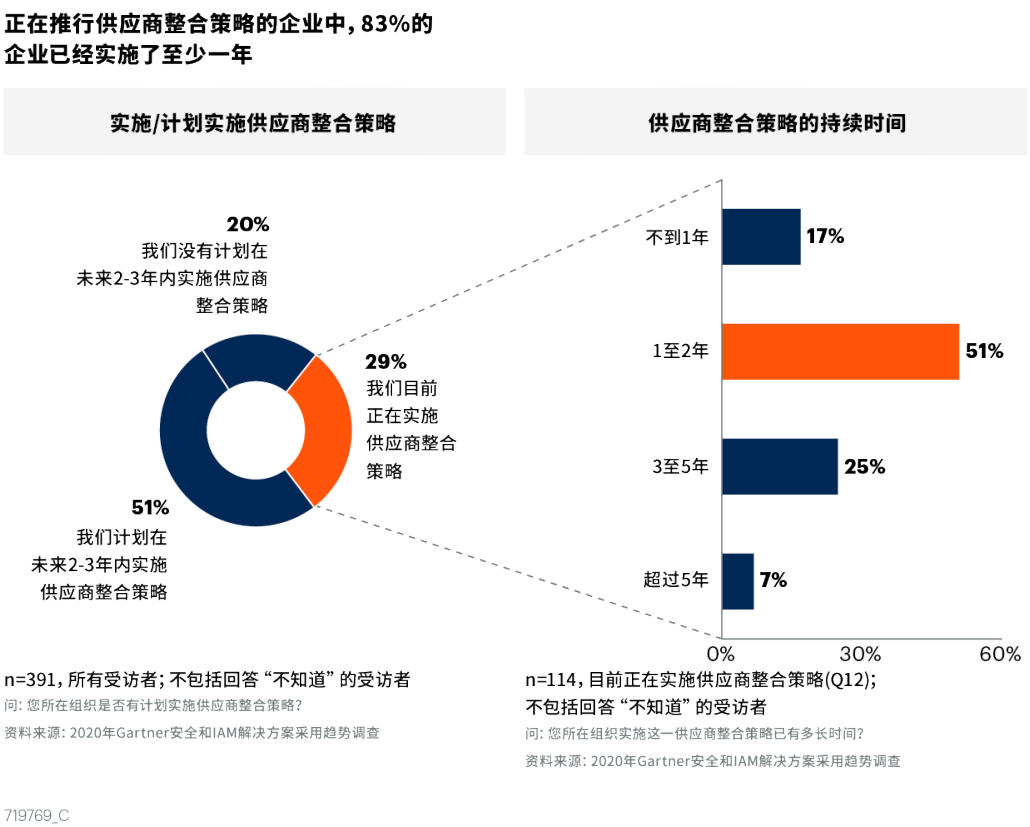
世界还面临着网络安全人才的巨大缺口-根据2020年ISC2的调查[1]，这一数字超过320万-因此运营效率是一个关键要求。有效的现代平台既注重业务和组织目标，也注重技术组合。此外，网络安全网的概念使这些平台能够使用现有和新兴的安全标准，通过API进行协作。管理可能是集中式的，而政策执行却是分布式的。

供应商正在采取两种明确的方式进行整合：

- **平台方式**
  - 利用相邻系统之间的相互依赖和共同点
  - 整合通用功能的控制台
  - 至少与同类最佳系统一样有效地支持组织的业务目标

图1

正在推行供应商整合策略的企业中，百分之八十三的企业已经实施了至少一年



- 整合和操作简单化意味着安全目标也得到了满足。

- **组合方式**
  - 在一个采购包中利用一组未整合或轻度整合的产品
  - 多个控制台，几乎没有或完全没有整合和协同作用
  - 经过供应商包装的传统方法
  - 不会实现任何承诺的整合优势

区分这些方式是套件效率的关键，供应商的营销总是说他们是一个平台。当您评估产品时，您必须考查是如何集成各控制台来管理和监控整合后平台的。同时，评估安全元素（如数据定义、恶意软件引擎）等如何无需重新定义即可重复使用，或能跨多个领域无缝应用。如果有多个控制台和多个定义，则应注意这是一个应该仔细评估的组合方式。

随着平台转移到云端进行管理、分析甚至交付，利用安全责任共担模型的能力给消费者带来了巨大的优势。然而，这将风险面扩大到了供应商，需要在第三方供应商管理中进一步恪尽职守。其优势包括：

- 没有物理技术债务；在切换供应商或技术之前没有硬件需要摊销。
- 减少或消除了关键技术对终端客户数据中心的占用。
- 运营任务（例如，补丁、升级、性能扩展和维护）由云提供商执行。系统得到全天候的维护和监控，供应商人员构成了终端客户人员配置的补充。
- 控制措施部署在靠近混合现代劳动力和分布式现代数据的地方；路径不会被迫通过客户拥有的任意地点进行过滤。

- 尽管是大型的目标，但云原生安全供应商规模够大，重点也比较明确，因此对基础设施的保障、管理和监测要优于大多数组织。

在供应商、能力和技术方面，整合工作遍布整个安全领域。在这里，我们强调网络安全与SSE平台的趋势、数据安全与新兴DSP的趋势、应用与云原生应用保护平台(CNAPP)的趋势，以及事件响应与XDR的趋势。

这些趋势涵盖了安全领域的不同方面，但即使在这里我们也能看到协同作用。例如，XDR可能会使用来自云访问安全代理(CASB)和其他SSE产品（以及直接来自流行的SaaS和云基础设施供应商）的数据以应对和管理云事件。DSP将提供SSE必须使用的数据分类，以防止云服务中未经授权的数据使用。同时，SSE和CNAPP市场都在纳入云安全态势管理(CSPM)。企业必须找到这些平台之间的边界，并确保它们的运行和管理方式保持一致-否则必须对其运行团队进行整合。

为了充分利用这一趋势，SRM领导者必须树立坚定自信的架构思维，而不是被动回应买方或成本驱动的供应商整合策略。这样有助于推动有意义的安全优化，并使您专注于对组织有利的特定领域。单纯地关注成本驱动策略往往会导致不太理想的安全选择和单一、固化的供应商结构。如果领导者能够评估运营或安全上的不足并推动整合投资，相比由安全团队推动的措施，建立安全保障的概率更高。

战略规划设想

战略规划设想： 到2025年，80%的企业将实现从单一供应商的安全服务边缘(SSE)平台统一网络、云服务和私人应用程序访问。

分析师： Neil MacDonald和Charlie Winckless

主要发现：

- 随着混合劳动力的出现，数据无处不在并可经各种设备访问，供应商正在提供集成式SSE解决方案以实现简单一致的网络、专用访问和SaaS应用安全。这些平台要管理由远程工作人员和分支机构发起的出站通信，并在离用户更近的地方（日益分布于企业网络之外）保护用户和数据。

- 为远程和分支机构用户提供的云交付安全服务将大部分运营负担转移给为此目的而配备的云安全服务，有助于更好地利用稀缺的安全人才。

- 企业需要从接入边缘安全中获得的业务成果在整个技术栈中是相似的。其中的关键是检测来自组织外部或内部的威胁，保护敏感数据，并确保无缝和高效的工作环境。

- 与同类最佳产品相比，单供应商解决方案实现的运营效率和安全效率更加显著，包括更精简的代理、更紧密的集成、更少的控制台，必须解密、检查和重新加密数据的位置也更少。

市场影响：

Gartner"工作的未来"研究表明，人力资源领导者预期会出现混合型的劳动力。我们对企业支出的持续评估显示，向云的迁移仍在继续。这两个趋势意味着，以数据中心为中心的传统网络和网络安全架构不仅相关性降低，而且在提供安全业务成果方面也不太有效。数据不在数据中心，数据的使用者也不在办公室。企业必须根据风险水平以适当的方式向数字劳动力提供各项功能的访问权限，并尽量降低对使用体验的影响。这就要求从云端提供网络安全服务，而不是通过虚拟专用网络(VPN)、软件定义广域网(SD-WAN)、MPLS或其他传输方式，将流量强行传送到客户在数据中心自有的安全堆栈。

远程工作模式和公共云服务的转变和采用早已开始，但新冠肺炎疫情加速了这一趋势的发展。SSE能够让组织使用以云为中心的方法来执行安全策略，随时为各个位置的远程工作者提供支持。SSE是降低复杂性、成本和供应商数量的直接方式。

安全网络网关(SWG)、CASB和零信任网络接入(ZTNA)产品在传统上是独立的市场，供应商直接也相互竞争。这些市场已经融合形成SSE市场，这三种能力是产品系列的基石，而远程浏览器隔离(RBI)、防火墙即服务(FWaaS)和数字体验监控(DEM)是关键的次级功能。

SSE可保证对Web、私人应用的访问和云服务的访问。其功能包括访问控制、威胁保护、数据安全、安全监控以及基于网络和API的集成所执行的可接受的使用控制。SSE主要以云端服务形式提供，可能包括本地或基于代理的组件。

未整合和近乎重叠的产品给管理员和用户带来的挑战是SSE市场发展的推动因素之一。这些挑战包括需要多个代理、不一致的安全结果、不同的用户体验，以及需要配置、支持和管理不同的安全产品来实现相同的结果。为改变这种不可持续的情况，CASB、SWG、ZTNA、RBI和FWaaS等多种控制措施被整合到SSE平台，无论在什么地方，都能够为用户提供强大、一致、自适应、适合风险的安全保障。它们通过管理SaaS的使用和控制对基础设施即服务(IaaS)的访问，使企业能够有效地使用新兴云技术。它们支持多种关键举措，如通过对连接实施身份和上下文控制来实现零信任。集成代理则可以在执行控制的同时减少端点的负载。最后，云交付的自适应安全方法可以有效地支持以"使用混合设备的混合劳动力"为特点的未来工作。

供应商正越来越多地收购或开发这些相邻的技术，并将其整合到一个单一的平台。通过减少控制台和配置平面的数量，并重新使用组件（如端点代理）和信息，可以最大化这种整合的效益。为迎合这种市场增长和兴趣，一些供应商将产品捆绑成一个没有任何协同作用的组合。从各种角度来说这都可能都是最糟糕的情况：产品可能在所有领域都不突出，也没有通过整合减少复杂性和开销。

在一个称为SASE的更广泛架构中，以云为中心的网络和网络安全模型将支持扩展至分支机构和旅行用户。相比在较小的站点部署安全堆栈，将互联网作为广域网并将流量输送到云安全堆栈可以带来巨大的优势。站点设备可以是现场可更换的单元，可以轻松接入SSE堆栈，并最大程度减少管理和维护。单一的执行控制平面（具有复制和高可用性的数据平面）简化了运营商的工作，特别是在同时使用紧密集成或有机SD-WAN供应商的情况下。

建议：

- 评估您的出站安全需求，以确定云管理的解决方案如何契合您的风险和业务情况。
- 通过评估供应商的可用SSE功能以及满足您最高要求的程度来确定其优先级。并非所有供应商都为每个独立的组件提供最佳的功能。这可能涉及不太成熟的云服务安全组件；薄弱的云基础设施足迹；缺少先进的数据安全功能；或缺乏对所有用例的全面ZTNA支持。
- 与网络团队合作，协调SSE服务的获取，以配合更广泛的网络转型、数字化举措和混合工作举措。

战略规划设想：到2025年，由于对更高级别的数据安全的需求被压抑，以及产品功能的迅速增加，30%的企业将采用DSP。

分析师：Joerg Fritsch和Brian Lowans

主要发现：

- 随着更多的网络安全点解决方案进入市场，SRM领导者已经达到了供应商整合和管理的关键点。他们必须合理安排他们的数据安全组合，以确定合并或同类最佳战略是否是正确的方法
- 由用例和特定于孤岛的数据安全控制措施组成的补丁让SRM领导者越来越困惑如何协调其能力和不足。
- 这种复杂性促使供应商迅速将不同的数据安全功能合并到数据安全平台中。通过应用这些新平台，组织可以更好、更轻松地保护他们的数据安全。
- 数据安全与大型产品平台的融合从未像现在这样明显，但复杂性的增长速度超过了供应商的整合速度。

市场影响：

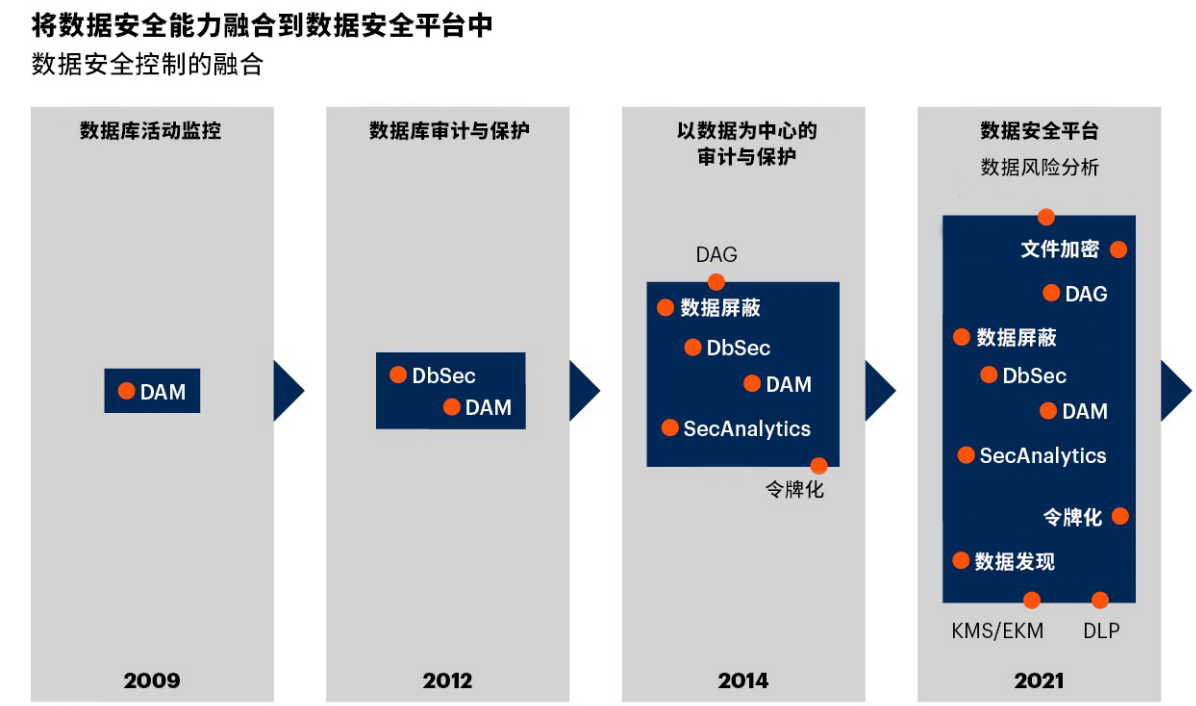
Gartner将DSP定义为以数据安全产品为特征的产品和服务，目标是整合不同数据类型、存储孤岛和生态系统的独特数据保护要求。数据安全市场的特点是供应商将其能力整合到DSP中。在这个市场上，以前孤立的能力将在一套共同的数据安全治理政策下聚集起来。这将大大简化数据安全工作，并使DSP成为推动有意义的数据风险分析、数据安全政策协调和简化运营的关键因素。

与数据安全、隐私和高级分析有关的两个趋势正在推动DSP的采用：

- 在加强数据安全和隐私方面，企业在DevSecOps、开放数据法规和高级分析的态度方面竞争日益激烈。
- 越来越多的组织数据开始在传统的数据中心之外，分布于不同的服务和信任边界。数据很可能在各种类型（基于基础设施、基于平台和SaaS）的公共云服务中进行处理和存储。这就要求企业对数据安全实施更有效的管理。

图2

将数据安全能力融合到数据安全平台中



资料来源：Gartner
748558_C

DSP显著加强了数据及其广泛用途的可见性和控制-例如，与未知行为有关，而不仅仅是与隐私有关的狭义合规目标。这使企业能够切实确保其数据安全。更高的可见性和控制提高了个人、组织和政府之间的数据流动的安全性（见图2）。这有助于做出更明智的决定，推动企业乃至整个社会的进步。

市场融合领域的示例包括：

- 数据保护技术（如令牌化、加密和数据屏蔽）、数据库活动监控(DAM)和数据发现。基于数据库代理、代理或网络网关的成熟DAM产品与数据屏蔽功能相结合，作为数据令牌化或加密后的一个后处理步骤。
- 数据屏蔽、数据发现、DAM和数据访问治理(DAG)。传统的数据屏蔽产品通过重建动态数据屏蔽网关的审计日志来增加DAM功能。增加数据发现功能是为了让客户可以更好地了解其数据存储。这些信息通常被存储在数据目录中。
- 数据发现和数据分类技术正与用户账户凭证结合使用，以创建数据风险分析并确定用户账户对特定数据集的访问权限。这种做法正越来越多地用于通过DAM、DAG和数据保护技术来执行数据安全治理政策。

建议：

- 清点数据安全控制措施，当您需要利用您的数据来支持现代数据安全平台时，孤立的数据安全工具会阻碍行动，因此您应该在几年的时间内逐步淘汰这些工具。
- 续签合同时，考虑合并供应商，以减少复杂性和成本。例如，在DAM、数据屏蔽、数据发现、数据加密或DAG方面。
- 通过选择提供高水平集成能力的DSP产品，将DSP纳入您的网络安全网状结构中。可组合企业的安全需要灵活的网络安全机制，在互操作性标准的基础上提供丰富的API集。

战略规划设想：到2025年，70%的企业将把保障云原生应用程序生命周期的供应商数量整合到最多三个供应商。

分析师：Neil MacDonald

主要发现：

- 鉴于云原生应用的独特特性，必须有一套复杂的、跨越开发和生产的重叠工具才能实施有效的保护。
- 使用多种分散的安全测试方法会增加复杂性、成本和发生错误配置、错误管理或错误的可能性。这削弱了应用程序的安全态势。
- 了解和解决云原生应用的真正风险需要先进的分析方法，结合应用定制代码风险、开源组件风险、云基础设施风险和运行时工作负载风险的各自独立的视图。
- 随着开发者采用无服务器PaaS，没有底层操作系统可供检测，并且越来越多地负责对包括基础设施在内的更多计算堆栈进行编程，复杂性问题变得更加严重。

市场影响：

为了支持数字业务举措，开发人员开始借助云原生应用开发。他们通常结合基于微服务的架构，这一架构使用容器构建，在DevOps风格的开发管道中组装，部署到程序化的云基础设施，并在运行时使用Kubernetes进行协调。理想情况下，它们是以不可改变的基础设施思维来维护的。这种转变给这些应用程序的安全带来了重大挑战。

最明显的是，企业用10个或更多不同的安全工具-有些是旧的，有些是新的-手动拼接了DevSecOps，每个工具都有各自的责任和应用风险视图。这导致了盲点和不完整的风险视图。

安全的云原生应用程序为企业提供了重新设计安全方法的机会。企业不应该把开发和运行环境当作单独的问题-用一系列单独的工具保障安全和扫描-而应该把安全和合规性作为跨越开发和运营的一个统一体。他们应尽可能地将工具整合到云原生应用保护平台中。

建议：

- 实施集成和融合的安全方法，涵盖云原生应用从开发到生产的整个生命周期。
- 随着CSPM和CWPP合同的到期，评估新兴的CNAPP产品，并利用这一机会降低复杂性和整合供应商。
- 将安全性整合到开发人员的工具链中，以便在代码创建和通过开发管道期间自动进行安全测试，减少采用时的摩擦。
- 要认识到没有完美的应用程序，并让开发人员重点关注严重性、可信度和风险度最高的漏洞上，以避免浪费开发人员的时间。
- 全面扫描所有开发工件和云配置，并将其与运行环境可见性和配置意识相结合，以确定风险补救的优先次序。

战略规划设想：到2027年，50%的中端市场安全买家将利用XDR来推动工作空间安全技术的整合，如端点、云和身份。

分析师：Peter Firstbrook

主要发现：

- 80%的SRM领导者希望整合安全供应商和产品，以更好地管理风险并提高安全运营效率。
- 保护人们使用的"工作空间"的安全工具，如端点、电子邮件和云SaaS应用程序，已经很成熟。这些安全工具之间的差异没有那么大，重点在于如何融入组织的安全运营。
- 拥有多种产品的大型安全技术供应商正越来越多地将其安全产品整合到通过通用数据平面和事件响应能力整合到一起的更广泛的解决方案中，通常称为XDR。
- XDR能力将成为买家在寻求战略解决方案时需要评估的一个日益重要的能力。

市场影响：

工作空间安全被定义为保护知识工作者使用的现代工作空间的安全工具的集合。工作空间安全的核心是端点保护平台(EPP)。然而，反钓鱼、SWG、CASB、远程访问工具、多因素身份验证(MFA)、数据丢失防护(DLP)和移动威胁防御(MTD)也是关键的工作空间安全工具。

传统上，买家为每个功能选择最佳的特定安全工具，然后使用安全信息和事件管理(SIEM)以及安全协调和自动响应(SOAR)工具来整合日志数据并执行调查和自动化操作。然而，主流CISO正在为这一类同类最佳安全堆栈的复杂性而苦恼。缺乏对综合风险态势的可见性和同类最佳工作空间安全堆栈的总拥有成本(TCO)是经常提到的问题。同时，拥有这些工具的广泛组合的解决方案供应商在集成方面往往不如他们的同类最佳对手产品。然而，这种情况正在改变。这种变化的一个关键推动因素是XDR。

尽管对什么是XDR存在争议，但出于本预测的目的，XDR被定义为跨多个安全产品提供通用检测、警报管理和事件响应能力的工具。XDR的目标是在多个安全工具之间实现更好的可见性，以及更快、更准确的事件响应，因为这些工具共享数据并与API集成，为多个工具提供半自动响应能力。

例如，如果端点代理被Metasploit攻破，凭证被盗并用于登录云应用程序，XDR可为事件响应者提供CASB信息，即凭证被用于云应用程序。然后，分析人员可以使用XDR功能触发自动化操作，撤销凭证并暂停云会话，并使用集成的CASB日志数据来确定泄露的程度。

建议：

负责工作空间安全的SRM领导者应该：

- 评估由XDR统一起来的工作空间安全包，作为降低安全运营复杂性的一种有意义的方式。
- 将EPP设计为XDR战略的基础，并以身份和电子邮件安全作为整合的首要任务，其次是云和网络安全。
- 考虑供应商组合中的数据和API集成，以及与选定合作伙伴的集成，作为一个关键考虑因素。
- 考虑工作空间安全工具在主动检测和补救可能被攻击者利用的配置问题方面的作用。

回顾

根据您的要求，我们回顾一下过去几年的部分关键预测。我们有意选择了两种对立的预测，即完全或大部分达到目标的预测，以及未达到目标的失误预测。

根据您的要求，我们回顾一下过去几年的部分关键预测。我们有意选择了两种对立的预测，即完全或大部分达到目标的预测，以及未达到目标的失误预测。

这个主题领域很新颖，很难有达到目标或失误的预测。

依据

[1] **2020年Gartner安全和IAM解决方案采用趋势调查：**此研究旨在了解哪些安全解决方案能使企业受益，以及哪些因素影响他们对这些解决方案的选择/偏好。研究采用网络调查形式，调查时间为2020年3月至4月，405名受访者分别来自北美、西欧和亚太地区(APAC)。选取的公司来自不同的行业，年收入低于5亿美元。受访者需为经理级或以上人员（不包括高管层），主要参与并负责企业的风险管理。

Gartner分析师与关注SRM的主要研究团队合作开展了这项研究。

[2] 络安全专业人员携手抵御疫情

资料来源：Gartner的研究G00758322, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 2021年12月1日

关于360数字安全集团

360数字安全集团(三六零数字安全科技集团有限公司)是数字安全的领导者，专注为国家、城市、大型企业、中小微企业提供数字安全服务。过去17年，360投入200亿，聚集超2000名安全专家，积累了2000PB安全大数据，基于以"看见"为核心的安全理念，凝练行业独有的高级安全威胁对抗实践，提出"1+4"数字安全框架模型，帮助城市、政府、企业数字安全体系的规划和建设数字安全体系，构建"摸清家底、感知风险、看见威胁、处置攻击、提升能力"5大安全能力，形成应对数字安全复杂威胁的完整能力。

面向各大管理部门，以SaaS化方式输出全网安全数据，提供数据赋能。目前，360全网数字安全大脑已捕获50个境外APT组织，检测到5200多次对我国20000多家重要机构单位的高级网络攻击事件。

面向大型企业，集中建设以数字安全大脑为核心的安全运营体系，云地一体、双脑协同，形成统一的风险感知、威胁发现、协同响应能力。目前已覆盖多数头部客户累计服务超10000家政企客户。

面向城市，把"卖药"模式升级为"数字安全医院"模式，建设城市级的看见、处置、指挥和防御能力，积极打造城市数字安全基地。目前已落地超20多个大中型城市，涵盖四大直辖市和部分省会城市，树立了标志性的城市级安全服务典范。

面向中小微企业，提供SaaS化的一站式安全云服务，实现从本地到远程、从终端到网络的硬件、软件、数据、行为、人的全方位安全管理。目前已被众多政府、企业、教育院校等各类单位采用，并在国内多个省份的重点供应链企业得到落地部署。

除此之外，360已连续七年支撑国家级网络攻防实战演习，一直是国家重大政治、经济活动的核心网络安全保障力量。在两会、十九大、九三阅兵、"一带一路"峰会、G20、金砖会议、APEC、七十周年庆典、2022年北京冬奥会等活动的重保工作，以及国家安全和国防安全相关工作中发挥了重要保障作用。